mindSHIFT Technologies, Inc.
47 CFR § 64.2009(e) CPNI Certification for 2017

This is the annual certification of mindSHIFT Technologies, Inc. (the "Company"), made in compliance with 47 C.F.R.§ 64.2009 (e), for 2018 covering the prior calendar year, 2017.

1. Date filed: March 1, 2018
2. Name of company(s) covered by this certification: mindSHIFT Technologies, Inc.
3. Form 499 Filer ID: 825979
4. Name of signatory: Joe Croft
5. Title of signatory: Chief Financial Officer
6. Certification:

I, Joe Croft, certify that I am an officer of the Company named above, and have personal knowledge that the Company has established operating procedures adequate to ensure compliance with the Commission's CPNI rules.

The accompanying statement explains how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken actions (i.e., proceedings instituted or petitions filed by the Company with state commissions, the court system, or the Commission against data brokers) against data brokers in the past year.

The Company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The Company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The Company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

mindSHIFT TECHNOLOGIES, INC.

Signed: _____
Joe Croft
Chief Financial Officer
Date: 3-1-18

Attachments: Accompanying Statement explaining CPNI procedures, with exhibit

mindSHIFT Technologies, Inc.
47 C.F.R. § 64.2009 (e) Certification for 2017

Accompanying Statement

Overview: In 2017, the Company distributed VoIP telephony services provided by its vendors to customers. The Company makes no certification with regard to its vendors' treatment of CPNI. To the extent the Company obtained access to CPNI in the ordinary course of its operations, it treated that information, for all purposes, as confidential information owned by the customer that engaged the Company to provide telephony services.

Employee Training and Discipline. The Company trains its employees concerning when they are and are not authorized to use confidential information, including CPNI, and required employees hired in 2017 to sign the summary of the FCC's CPNI Order attached to this statement and labeled as Exhibit A. The Company has entered into agreements with each of its employees and has instituted policies that expressly provide that employees who access, use or attempt to access or use confidential information, including CPNI, without authorization are subject to discipline, up to and including termination.

Sales and Marketing Campaigns. In 2017, the Company conducted no sales and marketing campaigns using CPNI. As such, the Company did not: (a) maintain a record of sales and marketing campaigns that used customers' CPNI; or (b) seek opt-in approval from customers for the use of their CPNI for marketing purposes.

Customer Authentication Methods. The Company has instituted and maintains appropriate authentication procedures to protect customers' confidential information, including CPNI, from unauthorized disclosure or use. Using these authentication procedures, the Company limits access to each customer's CPNI to the employees that the customer designates. Each request for access to systems and confidential information, including CPNI, is subject to those procedures and the Company's security policies. Each customer determines its own end-user access policies and precautions to prevent unauthorized access and use of its CPNI.

Customer Notification of CPNI Changes. As noted above, customers notify the Company of which customer employees are authorized to access and use the customer's confidential information, including its CPNI. In 2017, the Company provided, restricted or terminated access as each customer instructed and so notified each customer.

Notification to Law Enforcement and Customers of Unauthorized Access. In 2017, the Company continue to follow its policy of reporting access to, use of, or any attempt to access or use CPNI without authorization to law enforcement and to the customers affected. There were no such instances in 2017.

The Company took no actions against data brokers in 2017.

The Company received no reports or information indicating that any unauthorized access to or use of CPNI breaches occurred in 2017, and has such, has no records of any CPNI breaches discovered to retain.

Customer Complaints Regarding CPNI. In 2017:

1. The Company received no complaints from any source, including customers, of any incident

involving improper access to CPNI by its employees;

2. The Company received no complaints from any source, including customers, of any incident involving improper disclosure to CPNI by individuals not authorized to receive it;

3. The Company received no complaints from any source, including customers, of any incident involving improper access to online information by individuals not authorized to access that information; and

4. The Company was not aware of any effort to access, use or attempt to access or use any customer's CPNI without authorization.

mindSHIFT Technologies, Inc.
47 C.F.R. § 64.2009 (e) Certification for 2017

Accompanying Statement
Exhibit A

Employee Certification of Requirement to Comply with CPNI Regulations

This summarizes the Customer Proprietary Network Information ("[1]CPNI") Report and Order and Further Notice of Proposed Rulemaking ("CPNI Order") that the Federal Communications Commission ("FCC" or "Commission") released on April 2, 2007.[2] The CPNI Order modifies the rules for releasing and sharing CPNI, which also apply to providers of interconnected VoIP services. The memorandum lists the new requirements imposed by the CPNI Order.

CARRIER AUTHENTICATION REQUIREMENTS

Authentication Requirements for the Release of Call Detail Information[3]

- The FCC adopted new restrictions on the release of call detail information, which includes any information that pertains to the transmission of specific telephone calls, including
  - The number called (for outbound calls) or the number from which the call was placed (for inbound calls;
  - The time of the call;
  - The location of the call; and
  - The duration of the call.[4]
- Carriers are prohibited from releasing call detail information based on customer-initiated telephone contact except under three circumstances:
  - A carrier may provide call detail information if the customer provides the carrier with a pre-established password.
  - A carrier may initiate a call to the telephone number of record and disclose call detail information.
  - A carrier may, at the customer's request, send call detail information to the customer's address of record.
- If a customer is able to provide to the carrier, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call), then the carrier is permitted to proceed with routine customer care procedures.
  - Under these circumstances, carriers may not disclose to the customer any call detail information about the customer account, other than the call detail information that the customer provides, without the customer first providing a password.
- Although the FCC did not enact password protection for non-call detail CPNI, carriers remain subject to section 222's duties to protect CPNI, and thus carriers must authenticate a customer prior to disclosing non-call detail CPNI.
  - Carriers can determine the authentication method for the release of non-call detail CPNI that is appropriate for the information sought and consistent with their duties under section 222.

Password Requirements[5]

- Carriers may request that the customer establish a password at the time of service initiation.
  - Customers are not required to establish a password.
  - For existing customers to establish a password, a carrier must first authenticate the customer without the use of readily available biographical or account information.
    - "Readily available biographical information" includes such things as the customer's social security number, the customer's mother's maiden name, a home address, or date of birth.
    - "Account information" includes such things as account number or any component thereof, the telephone number associated with the account, or the amount of the last bill.
    - If a carrier already has password protection in place for an existing customer account, the carrier does not have to reinitialize the customer password.

Online Access to CPNI[6]

- Carriers are required to password protect online access to CPNI.
  - Carriers are prohibited from relying on readily available biographical or account information to authenticate a customer's identity before a customer accesses CPNI online.
  - A carrier must appropriately authenticate both new and existing customers seeking access to CPNI online.
    - Carriers are not required to reinitialize existing passwords for online accounts, but a carrier cannot base online access solely on readily available biographical or account information, or prompts for such information.
  - Carriers are allowed to create back-up customer authentication methods for lost or forgotten passwords in line with the back-up authentication methods established for customer-initiated telephone contact.
    - If a customer cannot provide a password or the proper response for the back-up authentication method to access an online account, the carrier must re-authenticate the customer prior to the customer gaining online access to CPNI.

Notification of Account Changes[7]

- Carriers are required to notify customers immediately of certain account changes, including changes to:Notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, as to reasonably ensure that the customer receives this notification.
  - Passwords;
  - customer response to a carrier designated backup means of authentication;
  - online account; or
  - address of record.

I have read and will adhere to the regulations contained herein.

Electronic Signature

Date

Accept

I authorize my Electronic Signature

[1] *Implementation of the telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rule Making, FCC 07-22 (rel. Apr. 2, 2007) (2007 CPNI Order).*
[2] *Id.*, ¶ 13.
[3] 47 C.F.R. § 64.2003(d).
[5] *2007 CPNI Order*, ¶ 15.
[6] *Id.*, ¶ 20.
[7] *Id.*, ¶ 24.